AUSA: Karen Reynolds Telephone: (313) 226-9672

AO 106 (Rev. 04/10) Application for a Search Warrant Special Agent: Elizabeth Weitzel Telephone: (313) 505-7304

UNITED STATES DISTRICT COURT

for the
Eastern District of Michigan

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* 201 E. Bennett Ferndale, MI 48220	Case: 2:22−mc−50974-1 Assigned To : Steeh, George Caram Case No. Assign. Date : 5/26/2022 Description: Search/Seizure Warrant (SO)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See ATTACHMENT A.

located in the Eastern District of Michigan, there is now concealed *(identify the person or describe the property to be seized)*:

See ATTACHMENT B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 1343, 18 U.S.C. 1341	Wire Fraud, Mail Fraud
18 U.S.C. 1028A	Aggravated Identity Theft

The application is based on these facts:

See attached AFFIDAVIT.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Elizabeth Weitzel
Applicant's signature

Special Agent Elizabeth Weitzel
Printed name and title

Sworn to before me and signed in my presence and/or by reliable electronic means.

Date: May 26, 2022

Jonathan J.C. Grey
Judge's signature

City and state: Detroit, MI

Jonathan J.C. Grey U. S. Magistrate Judge
Printed name and title

Affidavit in Support of an Application for a Search Warrant

I, Elizabeth Weitzel, being first duly sworn, hereby depose and state as follows:

Introduction and Agent Background

1. I make this affidavit in support of an application for a search warrant for evidence located at 201 E. Bennett, Ferndale, MI, 48220 **("SUBJECT PREMISES")** which is in the Eastern District of Michigan, as well as any computers, laptops, tablets, media storage, or cellphones found at this location for instrumentalities, fruits, and evidence of the violations of 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. §1028A (Aggravated Identity Theft), 18 U.S.C. §1341 (mail fraud), 18 U.S.C. § 1956 (Money Laundering), 18 U.S.C. § 641 (Theft of Government Funds) and conspiracy to commit the same and to seize evidence of such violations.

2. I am a Special Agent with the U.S. Department of Labor, Office of Inspector General, Labor Racketeering and Fraud (DOL-OIG/OI-LRF). I have been employed within the DOL since May of 2021. Prior to this assignment, I was a Special Agent with the United States Department of Housing and Urban Development Office of Inspector General (HUD OIG) for over 11 years. I am currently assigned to the Detroit Field Office of (DOL-OIG) and to the Detroit Metropolitan Identity Theft and Financial Crimes Task Force (DMIFT), led by the Federal Bureau of Investigation (FBI). My duties and responsibilities as a Task Force Officer include, but are not limited to, investigating violations of federal law, including Title 18, U.S.C. 1343 (Wire Fraud), Title 18, U.S.C. 1341 (Mail Fraud) and Title 18, U.S.C 641 (Theft of U.S Government money), Title 18, U.S.C. §1028A (Aggravated Identity Theft). I have conducted numerous criminal investigations involving Single-Family Loan Origination fraud, Home-Equity Conversion Mortgages, Public and Indian Housing Project Based Vouchers, Public Corruption, Fugitive Felon cases and financial and unemployment insurance fraud schemes. I was previously assigned to the Southeast Michigan Financial Crimes Task Force with the Michigan State Police and U.S. Secret Service where I conducted and led complex joint investigations pertaining to numerous violations of law relating to mortgage fraud and other financial crimes with other state and federal investigators. I have conducted and/or assisted on numerous search and arrest warrants related to these violations. I have additional experience and

training from the Federal Law Enforcement Training Center (FLETC) in the investigation of criminal activity, economic crimes, and identity theft. I am an "investigative or law enforcement officer" of the United States within the meaning of Title 5, U.S.C. § 8401 (17)(A)(i)(I).

3. Prior to my employment with HUD OIG, I was a Corporate Investigator and Bank Officer with Fifth Third Bank from July of 2006 until March of 2010. As a Corporate Investigator with Fifth Third Bank, I investigated cases involving mortgage fraud, wire fraud, consumer-loan fraud, counterfeit-check, identity theft, embezzlement, bank robberies, and various financial institution fraud.

4. As a Special Agent at the Department of Labor, I have conducted investigations into criminal violations of Title 29 and Title 18 of the United States Code. During this time, I have become familiar with and worked with Special Agents who have over 30 years of law enforcement experience investigating criminal schemes targeting Pandemic Unemployment Assistance (PUA) funds through the filing of false fictitious Unemployment Insurance (UI) Claims. Based on my direct personal experience with these cases, I have become familiar with the methods that criminals use to attack and exploit UI systems as well as tools and methods criminals often utilize to facilitate the fraud.

5. I make this affidavit based upon my personal involvement in the subject criminal investigation, my training and experience, and information provided to me by other law enforcement officers, agents and witnesses, including investigators with the State of Michigan's Department of Labor and Economic Opportunity. The information set forth below is based on a multitude of sources including, but not limited to, the review of records including financial, internet service provider, utility records; records from State of Michigan's (SOM) Unemployment Insurance Agency (UIA) regarding UI claims, and records from State of California Employment Development Department (EDD) regarding UI claims, documents, and government databases. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that criminal violations of 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. §1028A (Aggravated Identity Theft), 18 U.S.C. §1341 (mail fraud), 18 U.S.C. § 1956 (Money Laundering), 18 U.S.C. § 641 (Theft of Government Funds) and conspiracy to commit the same, have been committed by **LEAH BENNETT**, **SOPHIE MICHALAK**, and others in connection with unemployment insurance claims. There is further probable cause to believe that evidence of those crimes will be found at **SUBJECT PREMISES**. Based on my training and experience, people leave phones, devices, documents, mail, cash, computers, storage devices and other similar items in their vehicles. It is likely evidence of these crimes may be in vehicles at the **SUBJECT PREMISES**.

Summary

7. This is a joint investigation being conducted by the DOL OIG, FBI and United States Postal Inspection Service (USPIS). In February of 2021, DOL OIG Detroit Field office received a referral from the DOL OIG Los Angeles office that determined multiple Pandemic Unemployment Assistance (PUA) claims were filed with the California State Workforce Agency from Internet Protocol (IP) address **98.243.36.72**. A review of the IP address revealed that it was a static IP address in the Eastern District of Michigan. The investigation has shown that between July 2020 and September 2020, outside actors used this distinct IP address **98.243.36.72** to file over 91 fraudulent PUA claims with the California State Workforce Agency, resulting in the disbursement of over $1 million dollars earmarked for PUA benefit payments through interstate wire transfers. The investigation has shown that most of the PUA/UI benefits disbursed on these California claims were used in the Eastern District of Michigan, including but not limited to, local ATM withdrawals, hotel stays, and phone bill services.

Unemployment Insurance-Background & COVID 19

8. The Social Security Act of 1935 initiated the federal and state unemployment insurance system. The system provides benefits to individuals who are unemployed for reasons beyond their control. The purpose of the UI system is to lessen the effects of unemployment through cash payments made directly to laid-off workers, and to ensure that life necessities are met on a weekly basis while the worker seeks employment. In Michigan, the UI system is administered by the

Unemployment Insurance Agency (UIA), which is part of the State of Michigan's Department of Labor and Economic Opportunity. In the State of California, the Employment Development Department (EDD) administers the UI program.

9. On March 13, 2020, the President declared the ongoing Coronavirus Disease 2019 ("COVID-19") pandemic of sufficient severity and magnitude to warrant an emergency declaration for all states, tribes, territories, and the District of Columbia pursuant to section 501 (b) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. 5121-5207 (the "Stafford Act").

10. On March 18, 2020, the President signed the Families First Coronavirus Response Act ("FFCRA") into law. The FFCRA provides additional flexibility for state UI agencies and additional administrative funding to respond to the COVID-19 pandemic. The Coronavirus Aid, Relief, and Economic Security ("CARES") Act was signed into law on March 27, 2020. It expands states' ability to provide UI for many workers impacted by COVID-19, including for workers who are not ordinarily eligible for UI benefits. The CARES Act provided for three new UI programs: Pandemic Unemployment Assistance ("PUA"); Federal Pandemic Unemployment Compensation ("FPUC"); and Pandemic Emergency Unemployment Compensation ("PEUC").

11. The first program, PUA, provides for up to 39 weeks of benefits to individuals who are self-employed, seeking part-time employment, or otherwise would not qualify for regular UI or extended benefits under state or federal law or PEUC under section 2107 of the CARES Act. Coverage includes individuals who have exhausted all rights to regular UC or extended benefits under state or federal law or PEUC. Under the PUA provisions of the CARES Act, a person who is a business owner, self-employed worker, independent contractor, or gig worker can qualify for PUA benefits administered by EDD if he/she previously performed such work in California and is unemployed, partially unemployed, unable to work, or unavailable to work due to a COVID-19 related reason. A PUA claimant must answer various questions to establish his/her eligibility for PUA benefits. The claimant must provide his/her name, Social Security Number ("SSN"), and mailing address. The claimant must also identify a qualifying occupational status and COVID-19 related reason for being out of work. The eligible timeframe to receive PUA is from weeks of unemployment beginning on or after January 27, 2020 through December 31, 2020.

12. The second program, PEUC, provides for up to 13 weeks of benefits to individuals who have exhausted regular UI under state or federal law, have no rights to regular UI under any other state or federal law, are not receiving UI under the UI laws of Canada, and are able to work, and actively seeking work. However, states must offer flexibility in meeting the "actively seeking work" requirement if individuals are unable to search for work because of COVID-19, including because of illness, quarantine, or movement restriction. The eligible timeframe to receive PEUC is from weeks of unemployment beginning after the respective state has an established agreement with the federal government through December 31, 2020. The earliest being April 5, 2020.

13. The third program, FPUC, provides individuals who are collecting regular UI, PEUC, PUA, and several other forms of UC with an additional $600 per week. The eligible timeframe to receive PEUC was from weeks of unemployment beginning after the respective state had an established agreement with the federal government through July 31, 2020. The earliest being April 5, 2020.

14. On August 8, 2020, after FPUC expired, the President signed a Presidential Memorandum authorizing FEMA to use disaster relief funds pursuant to Section 408 Other Needs Assistance of the Stafford Act to provide supplemental payments for lost wages to help ease the financial burden on individuals who were unemployed because of COVID-19. The "Lost Wages Assistance Program" ("LWAP") served as a temporary measure to provide an additional $300 per week via a total of $44 billion in FEMA funds. The period of assistance for LWAP is August 1, 2020 to December 27, 2020, or termination of the program, whichever is sooner.

15. In total, more than $300 billion in additional federal funds for UI have been appropriated in 2020.

16. In California, a UI claim can be filed online on the EDD website. When an individual files a UI claim, the EDD automatically maintains certain information regarding the filing of the claim. This information includes the date and time the claim was submitted, the name of the person for whom the claim was

filed, and the IP address of the computer, or ISP account, that was used to file the claim.

17. UI claimants must answer various questions to establish their eligibility for UI benefits. Claimants must provide their name, Social Security Number, and mailing address. The claimants must also identify a qualifying occupational status and/or COVID-19 related reason for being out of work.

18. After EDD accepts a UI claim, EDD typically deposits UI funds every two weeks to an Electronic Bill Payment ("EBP") debit card administered by Bank of America, which claimants can use to pay for their expenses. The EBP card is sent via the U.S. Postal Service to the claimant at the address the claimant provides in their UI claim. Claimants can activate their debit card over the phone or online. To activate a card, a claimant must create a Bank of America unemployment user profile, which captures certain data including, but not limited to, the EDD claim number, claimant SSN, address where card was mailed. Each debit card includes the name of the beneficiary embossed or printed on the card's face.

19. Unemployment benefits are loaded onto the debit card electronically; or through the claimants provided bank account number, where the benefits are directly deposited to that bank account, through electronic funds transfers (EFTs). The EFTs originate from one or more accounts maintained by the Michigan UIA at Bank of America, a financial institution as defined by 18 U.S.C § 20.

20. Bank of America outsources the processing of transactions on UI prepaid cards to a vendor, Visa DPS [note "DPS" stands for debit processing solutions.] Visa DPS has two platform processor data centers that house all the UI prepaid card data for the Bank. The data centers are in Ashburn, Virginia and Highland Ranch, Colorado. Any transaction made on a prepaid card, including loading of funds, POS transactions, and ATM withdrawals, passes through one of these two data processor centers.

21. UI prepaid cards are mailed from one of five locations all located outside of the State of Michigan.

22. When receiving regular UI benefits, claimants must complete a Continued Claim Form (DE 4581) and certify every two weeks, under penalty of perjury, that they remain unemployed and eligible to receive UI benefits. EDD authorizes and deposits payment to the EBP debit card after it receives the Continued Claim Form. On or about April 23, 2020, California Secretary of Labor Julie Su directed the EDD to temporarily suspend the requirement for UI claimants to provide unemployment certifications (Continued Claim Forms) to prevent any unnecessary delays in dispensing benefit payments.

23. When the EDD needs to verify the identity of the claimant, an "ID Alert" is issued on a UI claim. When an ID Alert has been issued, the EDD sends the claimant a Request for Information (Form DE 1326E). The claimant must provide one of the following examples to prove identity verification: clear copy of a government-issued ID and social security verification. With this information, the EDD will determine the claimant's eligibility for UI benefits. The reasons why the claimant may be ineligible for UI benefits due to one of the following: (a) Claimant did not respond to the DE 1326E; or (b) Documents provided were not clear to make an eligible determination; or (c) Documents provided were insufficient and did not prove the claimant's identity.

24. Based on my training and experience, I know that criminal actors manipulate the UI systems to obtain fraudulent benefits by filing dozens of claims at a time, in the names of multiple individuals. This results in the distribution of numerous BOA debit cards loaded with PUA funds. To obtain cash from the cards, fraudsters often "dump" or "unload" ATM cards in sessions. For example, a fraudster will pull up to an ATM and unload or withdraw all the funds from multiple UI cards in rapid succession, obtaining large sums of money.

25. Furthermore, based on my training and experience, I know that criminal actors often defraud the UI program by using stolen personally identifiable information ("PII") to file UI claims and conspire with other criminal actors to obtain stolen identities or to file fraudulent UI claims.

Probable Cause

26. In February of 2021, the DOL OIG received allegations involving a fraud scheme aimed at defrauding the government of over a million dollars earmarked for PUA. DOL OIG Agents recognized this activity as they have investigated similar schemes since the onset of the pandemic in the spring of 2020. The scheme works through the online submission of false claims by outsiders targeting UI systems. The criminal actors manipulate the UI systems to obtain fraudulent benefits by filing dozens of claims at a time, in the names of multiple individuals.

27. In this instance, Agents identified one static IP address, **98.243.36.72,** which was responsible for filing over 91 PUA claims between July 2020 and September 2020. To date, these claims have resulted in the outlay of over $1 million in PUA benefits through the U.S. Mail and through wire transfers utilizing the nations' electronic financial infrastructure.

28. Based on my training and experience and through discussions with other seasoned agents in my office, I know over 91 PUA claims originating from one distinct IP address is indicia of a large-scale PUA fraud scheme.

IP 98.243.36.72 & the SUBJECT PREMISIS

29. Agents obtained records from Comcast that disclosed that IP **98.243.36.72,** was a static IP address assigned to the residence located at the **SUBJECT PREMISES**, within the EDMI. Comcast records showed that the account was held in the name of **SOPHIE MICHALAK** with a contact phone number of (248) 250-4170, with a start of service date of 02/25/2020.

30. Agents conducted physical surveillance of the **SUBJECT PREMISES** and noted that it appeared to be a single-family residence and not any kind of storefront or commercial location that would have reason to file dozens of claims for PUA

31. Agents also obtained DTE records for the **SUBJECT PREMISES**, which showed that account was held in the name of **SOPHIE MICHALAK**. Agents noted similarities to the Comcast records as telephone number (248) 250-

4170 was listed for **MICHALAK**. DTE records also listed an email address for **MICHALAK** as sophiemichalak1995@gmail.com.

32. DTE records also reported that **SOPHIE MICHALAK** has had active residential service at the **SUBJECT PREMISES** since 3/8/2020 and did not have active service at any other residence during the time of the investigation.

33. DTE payment records reported that **SOPHIE MICHALAK** made payments to the DTE account for the **SUBJECT PREMISES** using a Huntington Bank checking account ending in 7880, between 04/19/2020-03/31/2022.

34. DOL records show that over 91 claims were filed with the California State Workforce Agency by **IP 98.243.36.72** which resulted in the outlay of approximately $1.4 million in PUA benefits.

35. Agents conducted an additional query within DOL databases of **IP 98.243.36.72,** which identified a State of Michigan PUA claim, filed from that same IP address, under the name **LEAH BENETT**, as detailed below.

LEAH BENNETTS SOM PUA Claim

36. Agents obtained records from SOM UIA that reported on May 28, 2020 **LEAH H BENNETT**, DOB: 03/22/1996 filed a PUA claim from IP **98.243.36.72** with the telephone number, (734) 660-8022, and State ID Number B 530 493 302 232. **BENNETT** also provided the **SUBJECT PREMISES** as her claimant mailing address and residence.

37. **LEAH BENNETT** selected to receive her SOM PUA funds via direct deposit into her DFCU Financial account ending in 9924.

38. Agents obtained records from DFCU Financial for account ending in 9924. The **SUBJECT PREMISES** is listed on **LEAH BENNETT's** DFCU Financial Statements for DFCU accounts ending in 9924, 9932, and 9940.

39. Agents obtained records from DFCU Financial for account ending in 9924, 9932, and 9940 that reported payroll deposits from GP HOLDINGS LLC, which noted physical addresses at 6875 Gratiot Ave. Detroit, MI and 5245 Berwick Drive, Troy, MI. The checks were issued payable to **LEAH BENNETT** at the **SUBJECT PREMISES**.

Michigan and California PUA Claims filed with the SUBJECT PREMESIS

40. Between July 12, 2020 and July 17, 2020, three California State PUA claims were filed from **IP 98.243.36.72** listing the **SUBJECT PREMISES** as the claimants mailing address:

STATE_ID	CLMNT_NM	CLMNT_DOB	CLM_FILED	CLM_IP	CLMNT_MAILADDR
MI	LEAH, BENNETT	03/22/1996	May 28, 2020	98.243.36.72	201 E BENNETT AVE FERNDALE MI 48220
CA	C.J	05/16/1991	July 12, 2020	98.243.36.72	201 E BENNETT AVE FERNDALE MI 48220
CA	J.J	11/23/1989	July 16, 2020	98.243.36.72	201 E BENNETT AVE FERNDALE MI 48220
CA	A.G	04/06/1997	July 17, 2020	98.243.36.72	201 E BENNETT AVE FERNDALE MI 48220

Interview of UI Claimant C.J. Confirms UI Claimant is a Victim of ID Theft

41. On 11/23/2021, FBI SA Matt Schuff telephonically interviewed C.J. who stated that he/she never filed an unemployment claim nor did anyone file one his/her behalf in the State of California. C.J was unfamiliar with the email address CJACK0979@gmail.com. C.J. further reported that they had only ever lived in New Mexico and Arizona.

Nexus to the SUBJECT PREMISES

42. On 04/06/2022, Agents obtained **LEAH BENETT's** current driver's license, which listed her address as the **SUBJECT PREMISES**.

43. On 04/06/2022, Agents obtained information from the Michigan Secretary of State Records, confirming a Chevrolet Malibu, with TAG #DJQ6531 is registered to **LEAH BENNETT** at the **SUBJECT PREMISES**.

44. On 05/13/2021, the FBI conducted surveillance at the **SUBJECT PREMESIS**, and identified **MICHALAK** leave the **SUBJECT PREMISIS** and enter the dark colored Honda Civic parked at the residence, bearing the TAG # DAQ2354.

45. On 04/12/2022, I conducted surveillance at the **SUBJECT PREMISES** and observed **LEAH BENNETT** exit the **SUBJECT PREMISES** and get into her 2018 Chevrolet Malibu, with TAG # DJQ6531. I also observed a Honda Civic, bearing the TAG # DAQ2354 parked in front of the **SUBJECT PREMISES.**

46. Subsequent queries of the Honda Civic bearing the TAG# DAQ2354 indicated that vehicle was registered to James Stanley Michalak, who is assumed a family member of **MICHALAK**/possibly her father.

47. Bank records for **LEAH BENNETT's** accounts at DFCU listed the **SUBJECT PREMISES** as her address.

48. DTE utility records for the **SUBJECT PREMISES** list **SOPHIE MICHALAK** as the account holder.

SOPHIE MICHALAK Potential Co-Conspirator

49. As indicated above, **MICHALAK** has been identified as living at the **SUBJECT PREMESIS**, and maintained utility records in her name at the **SUBJECT PREMESIS**, during the time the above-mentioned claims were filed utilizing the **SUBJECT PREMESIS** address.

50. I conducted an open-source review of Facebook accounts associated with **BENNETT** and **MICHALAK**, which confirmed they are friends on Facebook and had numerous other friends in common.

51. Based on my training and experience, and the information obtained at this stage of the investigation, I believe that **MICHALAK** may be involved in the scheme; because numerous PUA/UI claims were filed using her address; and the fact that **MICHALAK** and **BENNETT** have multiple other friends and associates in common. Therefore, I have reason to believe that a search of **MICHALAK's** person and vehicles may yield evidence of the violations under investigation.

Other Investigative Steps and Knowledge

52. Based upon my training and experience in mail fraud and identity theft investigations, I know that suspects often take the mail and bankcards that they obtained illegally to their residences so they can open, examine, and exploit them in private. I also know that these same suspects often store the contents of illegally obtained mail at their residences and in their vehicles until they are ready or while they are continuing to use them.

53. I am also aware that individuals involved in mail fraud, access device fraud, aggravated identity theft, and conspiracy to commit such offenses (including schemes to acquire and to use federally insured bank credit cards assigned to others), obtain access devices, PIN numbers, financial information, identity information, checks and other personal and financial information of victims via fraud and theft. I am also aware that in mail fraud and identity theft schemes, perpetrators will keep tools, implements, financial statements, access devices, and stolen items close to themselves (especially in vehicles they use, or their person, in their residences, in the residences of extended family members, and in storage units) or in areas to which they have access in order to ensure custody and control of the items and for easy access for use or disposal.

Use of Electronic Devices for Criminal Activity and Forensic Analysis

54. Based on the above-described evidence, there is probable cause to believe that the Subject used electronic devices—such as smart phones, cell phones, tablets, and computers as instrumentalities of their scheme and used the devices to store evidence and fruits of their crimes.

55. As described above, many of the fraudulent access devices were registered via the internet, and, in some instances, a phone number or email address was provided. These actions typically require the use of electronic devices.

56. Additionally, the stored communications and files connected to an electronic device may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. There is probable cause to believe the stored communications and files within

electronic devices contain communications and other files and data that are evidence of the offenses described in this affidavit.

57. In my training and experience, evidence of who was using an electronic device and from where, and evidence related to criminal activity of the kind described above, may be found in the various files and records described in this affidavit. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

58. Additionally, the electronic device user's account activity, logs, stored electronic communications, and other data can indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

59. There is probable cause to believe that electronic device activity will also provide relevant insight into the owner's state of mind as it relates to the offenses under investigation. For example, information on the device may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information to conceal evidence from law enforcement).

60. Additionally, as described in this affidavit, there is probable cause to believe the offenses may involve one or more co-conspirators in locations scattered around the U.S. Based on my training and experience, such conspirators must use electronic means to communicate about the scheme and to share large amounts of data related to the scheme such as the personally identifiable information of victims. Based upon my training and experience, my conversations with other law enforcement personnel assisting in this case, and my investigation in this case, I am

also aware that persons involved in identity theft, mail theft, access device fraud, and bank fraud, along with their conspirators/accomplices use smart phones, cell phones, tablets, and computer laptops to communicate with one another, either by voice calls, emails, or text messages regarding their fraud and theft activities. I know that perpetrators who use such devices commonly exchange real time information about theft and fraud activity and other information regarding execution of theft or fraudulent transactions. Such information can be found stored in the text/email messages and images on such devices. Such persons also use the devices to link with the internet to obtain addresses and maps and locations/addresses of victims, including but not limited to merchants, banks, and individual identity theft victims. Such devices can also be used to: remotely make online fraudulent purchases, perform false or fraudulent mobile banking operations and checks (verifications), and distribute the proceeds of fraudulent activities to co-conspirators via banking and money-transfer applications.

61. Based upon my training and experience, my conversations with other law enforcement personnel assisting in this case, and my investigation in this case, I am aware that the complete contents of text messages, image files, and emails may be important to establishing the actual user who has dominion and control of a particular phone or computer at a given time. Cell phones may be subscribed to under false names with little to no verification by the service provider. Cell phones and computers may also be used by multiple people. Given the ease with which such items may be obtained and used, and the rarity with which law enforcement has eyewitness testimony about a defendant's use of a particular cell phone or device that was used to send a particular text or email message, investigators often have to rely on circumstantial evidence to show that an individual was the actual user of a particular cell phone or device. Often, by piecing together information contained in the contents of the device (cell phone or computer or storage device) an investigator can establish the identity of the actual user. Often, those pieces will come from a time before the device was used in criminal activity. Limiting the scope of the search for information showing the actual user of the device would, in some instances, prevent the government from identifying the user of the device and, in other instances, allow a defendant to possibly suggest that someone else was responsible. Therefore, the entire content of a communication device often provides important evidence regarding the actual user's dominion and control of the device. Moreover, review of the contents of communications of electronic

storage devices, including text and email messages sent or received by the subject device assist in determining whether other individuals had access to the device.

62. Based upon my training and experience, my conversations with other law enforcement personnel assisting in this case, and my investigation in this case, I am aware that criminals discussing their criminal activity via electronic communication devices (email and text messaging) may use images, slang, short forms (abbreviated words or phrases such as "lol" to express "laugh out loud"), or code words (which require entire strings or series of text message conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. It is even possible to use pictures, images, and emoticons (images used to express a concept or idea such as a happy face inserted into the content of a text message or the manipulation and combination of keys on the computer keyboard to convey an idea, such as the use of a colon and paren :) to convey a smile or agreement) to discuss matters. "Keyword searches" or other automated methods of review of the text messages sent to and from the subject device would not account for any of these possibilities, so actual review of the text and email messages by law enforcement personnel with information regarding the identified criminal activity is necessary to find all relevant evidence.

63. Based upon my training and experience, my conversations with other law enforcement personnel assisting in this case, and my investigation in this case, I have learned the following additional information:

a. Individuals who steal, misdirect, take, unlawfully possess, or by fraud or deception obtain, U.S. Mail often maintain the U.S. Mail, and its contents – including access devices, bankcards, and gift cards – for long periods of time to exceed months. Such individuals will also scan onto computers, cell phones, and computer storage devices stolen mail or fraudulently obtained mail (and its contents) and maintain on computers, cell phones, and storage devices co-conspirators names, victim's names, addresses (of victims, associates, accomplices), and stolen means of identification, to include images of such, thereby reducing such items' exposure to law enforcement and the community. Individuals use their cell phones and personal computers to make online purchases using gift cards to order items that will be shipped to their residences.

b. I am aware that even if a perpetrator deletes evidence of criminal activity (such as identity theft, and fraudulent use of financial information in U.S. Mail) from electronic storage devices, the evidence often can be recovered from the devices, including computers or other forms of electronic storage media.

64. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period on the device. This information can sometimes be recovered with forensics tools.

65. As described above and in Attachment B, this application seeks permission to search for records that might be found on the **SUBJECT PREMISES**, in whatever form they are found. One form in which the records might be found is data stored on an electronic device's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic devices and storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

66. There is probable cause to believe that things that were once stored on any electronic devices located at any of the **SUBJECT PREMISES** may still be stored there, for at least the following reasons: a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space-that is, in space on the storage medium that is not currently being used by an active file-for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. c. Wholly apart from user-generated files, computer storage media-in particular, computers' internal hard drives-contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts

from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information. d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

67. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how electronic devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the electronic devices found because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic

process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

f. I know that when an individual uses an electronic device, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain data that is evidence of how the electronic device was used, data that was sent or received, and other records that indicate the nature of the offense

68. **Necessity of seizing or copying entire computers or storage media.**

In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. **The time required for an examination.**

As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely

that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. **Technical requirements.**

Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. **Types of electronic media.**

Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

69. **Nature of examination.**

Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of electronic devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a device to human inspection to determine whether it is evidence described by the warrant.

70. **Manner of execution.**

Because this portion of the warrant—seeking forensic examination of electronic devices found—seeks only permission to examine device(s) that would be already in law enforcement's possession, the execution of the forensic examination would not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the court to authorize execution of such examination at any time in the day or night following the seizure of the device.

Biometrics

71. The warrant I am applying for would permit law enforcement to obtain from **LEAH BENNETT** and **SOPHIE MICHALAK,** the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices, and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.

d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

e. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

g. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the subject premises and reasonably believed by law enforcement to be a user of the device, to the fingerprint scanner of the device; (2) hold the device in front of the face of those same individuals and activate the facial recognition feature, for the purpose of

attempting to unlock the device in order to search its contents as authorized by this warrant.

72. Because several people may share the addresses listed in Attachment A as a residence, it is possible that the location will contain electronic devices and storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is probable that the things described in this warrant could be found on any of those devices or storage media, the warrant applied for would permit the seizure and review of those items as well.

Conclusion

73. Based on the forgoing, there is probable cause to believe that evidence of the violations of 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. §1028A (Aggravated Identity Theft), 18 U.S.C. §1341 (mail fraud), 18 U.S.C. § 1956 (Money Laundering), 18 U.S.C. § 641 (Theft of Government Funds) and conspiracy to commit the same and to seize evidence of such violations, are likely contained in various devices and storage media, and in other locations further described in Attachment A. By this affidavit and application, I request the Court issue a search warrant for the **SUBJECT PREMISES** including vehicles associated with the **SUBJECT PREMISES**, allowing agents to seize and search the items further described in Attachment B. Additionally, I request authority to search **LEAH BENNETT** and **SOPHIE MICHALAK's** person in case **BENNETT** and **MICHALAK** have digital devices on her person and are located outside of the residence at the time the search warrant is executed, allowing agents to seize and search the items further described in Attachment B.

74. Additionally, as described in Attachment B, the affiant requests the authority for law enforcement officers executing this warrant to compel **LEAH BENNETT** and **SOPHIE MICHALAK** to provide law enforcement officers the means to unlock any digital devices seized during the execution for this warrant, to include passcodes, digital patterns, direction lock codes, the use of **LEAH BENNETT** and **SOPHIE MICHALAK's** fingerprints, picture of their face or other biometrics which may be required to access their devices.

REQUEST FOR SEALING

75. It is respectfully requested that this court issue an order sealing, until further order of the court, all papers submitted in support of this application, including the

application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all the targets of this investigation will be search at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully Submitted,

Elizabeth Weitzel

Elizabeth Weitzel, Special Agent
U.S. Department of Labor – OIG

Sworn to before me and signed in my presence
and/or by reliable electronic means.

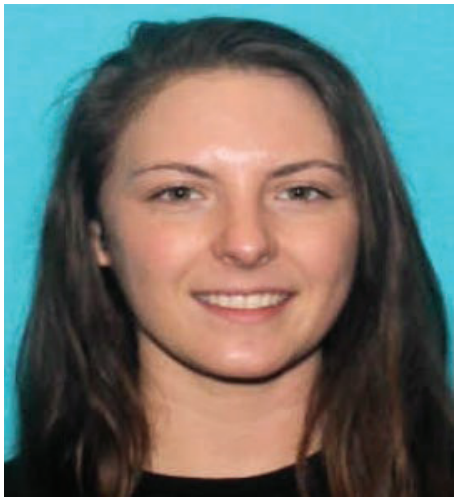
Jonathan JC Grey

HON. JONATHAN J.C. GREY
United States Magistrate Judge
Date: May 26, 2022

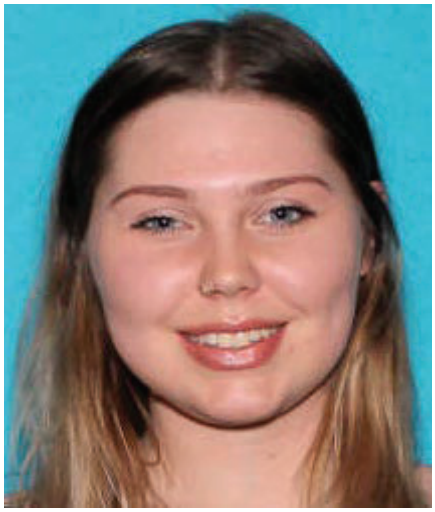
Attachment A

Property to Be Searched

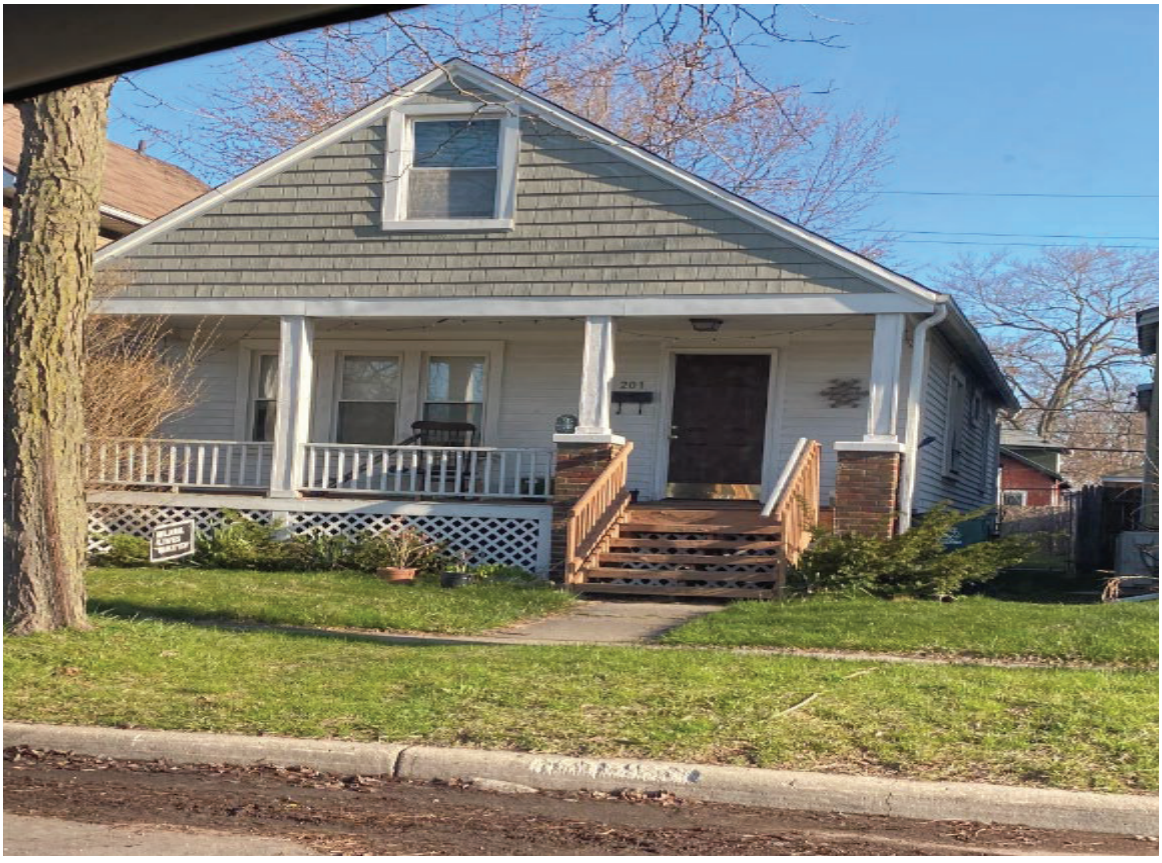
LEAH H. BENNETT, is a white female with date of birth 03/22/1996 and SSN:XXX-XX-8373. **BENNETT's** photograph is provided below:



SOPHIE E. MICHALAK, is a white female with date of birth 12/11/1995 and SSN: XXX-XX- 5157. **MICHALAK's** photograph is provided below:



The property to be searched is the residence located at: 201 E. Bennett, Ferndale, MI, 48220 (**SUBJECT PREMISES**). The **SUBJECT PREMISES** is a single-family residence/ bungalow with light colored siding, and an open porch with lights near the eaves, and a dark colored door with a brass kick-plate. The numbers "201" are mounted on the house above the mailbox, to the left of the front door. The residence does not appear to have a driveway or a garage associated with the residence. A photo of the property to be searched was obtained by the Affiant and included below:



This warrant authorizes the on- or off-site forensic examination of electronic devices found at the searched location for the purpose of identifying the electronically stored information described in Attachment B.

Attachment B

Materials that constitute evidence of the commission of criminal offenses, or contraband, the fruits of crimes, or property designed or intended for use or which is or has been used as the means or committing criminal offense, namely the violations of 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. §1028A (Aggravated Identity Theft), 18 U.S.C. §1341 (mail fraud), 18 U.S.C. § 1956 (Money Laundering), 18 U.S.C. § 641 (Theft of Government Funds) and conspiracy to commit the same and to seize evidence of such violations including but not limited to the following:

• All unemployment insurance records and documents, including unemployment insurance statement of benefits and awards, continued claim forms, notification of claims filed, employer wages reported, and any correspondence to or from State Workforce Agency (SWA);

• All debit cards as well as any and all records and documents relating to debit cards, including transactional history, statements, or ATM receipts;

• All records, documents and communications pertaining to, and including, falsified, fictitious and/or stolen identifications or Personal Identifying Information, logs, journals, payment data, ledgers, tally sheets, receipts, files, folders, tax information, date books, falsified, fictitious and/or stolen identifications, personal identification numbers;

• All financial or bank records, documents, and communications related to unemployment insurance fraud schemes, including debit cards, credit cards, or stored value cards issued with respect to unemployment claims or capable of receiving payment from Michigan Unemployment Insurance Agency or any other SWA.

• Any items tending to establish the identity of persons who have dominion and control over the location, premises, or items to be seized, including delivered mail, whether inside the location or in the mailbox (or mailboxes), bills, utility bills, telephone bills, miscellaneous addressed mail, personal letters, personal identification, purchase receipts, rent receipts, sales receipts, tax statements, payroll check stubs, keys, and receipts for any safe deposit box (or boxes), keys and receipts for rental storage space, keys, and receipts for post office box or mail drop rentals, ignition keys, car door and trunk keys, vehicle ownership certificates or "pink slips," and/or vehicle

registration slips and photographs tending to show occupation of the residence/business and connections between coconspirators, whether identified, or unidentified.

• Books, records, receipts, bank statements and records, cancelled checks, loan documents, money drafts, letters of credit, money orders, wire transfers, and check receipts, passbooks and all other items evidencing the obtaining, secreting [i.e. safety deposit keys and records], transfer, and/or concealment of money. Agents are also authorized to open any safe found on the premises.

• All identification documents, including driver's license, social security cards, employee identification cards or badges, or other identification cards that tend to show possession of another individual's personal identification information.

• All documents showing where and when employees worked for a particular time.

• All records and documents containing names, social security numbers, dates of birth, addresses, telephone numbers, employers, and dates of hire and termination.

• All personal and business tax records including state, local, and federal tax returns together with all schedules and attachments, drafts, and copies of any returns, non-filed or partially completed returns, all tax forms and schedules, tax preparation files, work papers, correspondence, to/from any accountant, or return preparer.

• Paper, tickets, notices, vehicle rental receipts, hotel records, travel agency invoices and tickets, credit card receipts and invoices, travel schedules, records of long-distance telephone calls, passports, and/or records and other items relating to domestic and foreign travel. Airline tickets, airline ticket stubs, travel agency invoices and frequent flyer account documents.

• Records pertaining to the purchase and/or leasing of vehicles.

• Quantities of United States currency more than $1,000 or quantities of foreign, virtual, or internet currency or precious metals with a value in excess of $1,000 USD;

• Luxury or other items determined to have a value more than $200 including watches, jewelry, designer clothing and shoes, fur coats, sunglasses, purses, antiquities, and high-end liquor and champagne.

• As used above, the terms records or documents include records or documents created, modified, or stored in electronic or magnetic format and any data, image, or information that is capable of being read or interpreted by a computer. To search for any items that were prepared, modified, or stored in electronic or magnetic form, searching agents may seize and search the following:

• All records, documents and communications relating to the application for cellular telephone service in the names of any individuals or companies, including any correspondence, contracts, receipts, computer printouts, or cellular telephones.

• All SIM cards/SD cards related to cell phone network connections or storage.

• Computers, computer hardware, electronic devices, and computer-related equipment capable of storing information in electronic, optical or magnetic format, including, but not limited to, laptop computers, desktop computers, notebook computers, tablets, hard drives, central processing units, internal and peripheral storage devices, CD-ROMs, DVD- Roms, Zip disks, thumb drives, diskettes, fixed disks, tapes, smart cards, memory cards, memory sticks, cellular telephones, blackberries, electronic dialers, electronic notebooks, PDAs and passwords, password files, test keys, data security, encryption devices, keys or codes, physical keys, or dongles used to access the devices or used to access the computers to be searched or to convert any data, file or information on the computers/devices to a readable format.

• All electronically stored communications such as e-mail and text messages. Peripheral input/output devices (including but not limited to keyboards, printers, docking stations, video display monitors and related communication devices such as cables and connections). Computer equipment capable of printing, copying, or scanning documents or identifications, including, but not limited to, printers, scanners, copy machines, ink cartridges, toners and drivers for the equipment. Any software, documentation, operating logs, instruction manuals, used to

facilitate direct or indirect communication with the computers and devices to be searched.

• Computer software, hardware, or digital contents related to the sharing of internet access over wired or wireless networks allowing multiple persons to appear on the internet from the same IP address

• During the execution of the search of the locations described in Attachment A law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of **LEAH BENNETT** and **SOPHIE MICHALAK**, at the subject premises and to the fingerprint scanner of the devices(s) found at the premises; (2) hold the device(s) found at the premises in front of the face of those same individual and activate the facial recognition feature; and/or (3) hold the devices(s) found at the premises in front of the face of those same individuals and activate the iris recognition feature, for the purpose of attempting to unlock the device (s) to search the contents as authorized by this warrant.

• If computers or other digital devices are found in a running state, the investigator may acquire evidence from the devices prior to shutting the devices off. This acquisition may take several hours depending on the volume of data.

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets server computers, and network hardware. All the above will be seized for an off-site search for information, records, files, documents, photographs, e-mails, text messages and communications related to the UI fraud scheme.

AUSA: Karen Reynolds Telephone: (313) 226-9672

AO 93 (Rev. 11/13) Search and Seizure Warrant Special Agent: Elizabeth Weitzel Telephone: (313) 505-7304

UNITED STATES DISTRICT COURT

for the
Eastern District of Michigan

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* 201 E. Bennett Ferndale, MI 48220	)	Case: 2:22−mc−50974-1 Assigned To : Steeh, George Caram Case No. Assign. Date : 5/26/2022 Description: Search/Seizure Warrant (SO)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Michigan.
(identify the person or describe the property to be searched and give its location):

See ATTACHMENT A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See ATTACHMENT B.

YOU ARE COMMANDED to execute this warrant on or before June 8, 2022 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the presiding United States Magistrate Judge on duty.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: May 26, 2022 at 7:23 p.m.

Jonathan J.C. Grey
Judge's signature

City and state: Detroit, MI

Jonathan J.C. Grey U. S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title